



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,588	08/07/2001	Thomas E. Tahan	5181-75900	2724
7590	07/14/2006		EXAMINER	
Rory D. Rankin Conley, Rose, & Tayon, P.C. P.O. Box 398 Austin, TX 78767				SCHUBERT, KEVIN R
		ART UNIT		PAPER NUMBER
		2137		

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/923,588	TAHAN, THOMAS E.	
	Examiner Kevin Schubert	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 June 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-4, 6, 8, 10-21, 23, 25, 27-38, 40, 42 and 44-51 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-4, 6, 8, 10-21, 23, 25, 27-38, 40, 42, 44-51 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

Claims 1-4,6,8-21,23,25-38,40, and 42-51 have been considered.

Claim Rejections - 35 USC § 102

5 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

10 (e) the invention was described in (1) an application for patent; published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15

Claims 1-2,6,8,10,12,15-16,18-19,23,25,27,29,32-33,35-36,40,42,44,46, and 49-50 are rejected under 35 U.S.C. 102(e) as being anticipated by Bots, U.S. Patent Application No. 6,226,748.

20 As per claims 1,18, and 35, the applicant discloses a method of controlling information flow through a firewall comprising the following limitations which are met by Bots:

a) determining a first incoming packet community set (PCS) of a first data packet received on an interface of said firewall (Col 7, lines 1-6);

b) discarding said first data packet in response to detecting said PCS is not a subset of an

25 interface community set (IFCS) of said interface (Col 8, lines 2-4);

processing said first data packet in response to detecting said first incoming PCS is a subset of said IFCS, wherein said processing comprises:

c) matching said first data packet to a first rule of a plurality of rules of said firewall (Col 7, lines 1-19);

30 d) comparing said first incoming PCS to a second incoming PCS specified by the first rule (Col 7, lines 1-19);

Art Unit: 2137

e) changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS (Col 7, lines 1-19).

5 f) comparing said outgoing PCS with a destination community set of said first data packet, prior to transmitting the first data packet to said destination community (Col 7, line 56 to Col 8, line 14; Fig 4);

g) discarding said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set (Col 8, lines 2-4);

h) further processing said first data packet in response to detecting said outgoing PCS is a subset of said destination community set (Col 7, line 56 to Col 8, line 14);

10 i) wherein the determining, discarding, and processing are performed within a single node of a network (Col 7, line 56 to Col 8, line 14).

As per claims 2,10,19,27,36, and 44, the applicant discloses the method of claims 1,9,18,26,35, and 43, which are met by Bots, with the following limitation which is also met by Bots:

15 Wherein said determining comprises determining a source network address community set (NACS) of said first data packet (Col 6, lines 34-38; Col 7, lines 1-6).

As per claims 6,23, and 40, the applicant describes the method of claims 5,22, and 39, which are anticipated by Bots, with the following limitation which is also met by Bots:

20 Wherein said processing further comprises discarding the first data packet, in response to determining the first incoming PCS does not match the second incoming PCS (Col 7, lines 14-16).

As per claims 8,25, and 42, the applicant describes the method of claims 6,23, and 40, which are met by Bots, with the following limitation which is also met by Bots:

25 Wherein changing said first incoming PCS to the outgoing PCS is in further response to determining that said first rule includes the action of forwarding said first data packet (Col 7, lines 1-19).

Art Unit: 2137

As per claims 12,29, and 46, the applicant describes the method of claims 1,18, and 35, which are met by Bots, with the following limitations which are also met by Bots:

5 a) transmitting said first data packet via an output interface of said firewall in response to detecting said outgoing PCS is a subset of the interface community set (IFCS) of said output interface (Col 6, lines 34-46);

b) discarding said first data packet in response to detecting said second PCS is not a subset of said IFCS (Col 8, lines 2-4);

10 As per claims 15,32, and 49, the applicant describes the method of claims 1,18, and 35, which is met by Bots, with the following limitation which is also met by Bots:

Further comprising consulting a community information base (CIB) (Col 2, lines 62-65);

15 The community information base corresponds to lookup tables on the VPN units, which identify members of a group by their network addresses, provide services such as compression and encryption for authentication purposes, and include information corresponding to the VPN unit interfaces which allow the compression, encryption, and authentication rules of one VPN unit to be recognized by another.

As per claims 16,33, and 50, the applicant describes the method of claims 15,32, and 49, which are met by Bots, with the following limitation which is also met by Bots:

20 Wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces (Col 2, lines 62-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

25 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5 Claims 3,11,20,28,37, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable by Bots in view of McNeill, U.S. Patent No. 6,167,052.

As per claims 3,11,20,28,37, and 45, the applicant discloses the method of claim 1,9,18,26,35, and 43, which are anticipated by Bots, with the following additional limitation which is met by McNeill.

10 Wherein said determining comprises determining a source network service community set (NSCS) of said first data packet (McNeill: Abstract);

The applicant describes the NSCS as identifying the source and destination by link layer addressing or a similar layering protocol (Applicant: Page 26). Bots discloses all the limitations of claims 1,9,18,26,35, and 43 and the use of identifying a source by its address, but fails to disclose the use of 15 determining a source by link layer addressing or similar layering protocol. McNeill discloses a system similar to Bots' and the applicant's in which connectivity is established in a network based on source and destination link layer addresses. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of McNeill with those of Bots and determine a source and destination from link layering addressing as another means to determine the source and destination of a 20 data packet.

Claims 4,13,21,30,38, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable by Bots in view of Kidambi, U.S. Patent No. 6,424,626.

25 As per claims 4,13,21,30,38, and 47, the applicant discloses the method of claims 1,12,18,29,35, and 46, which are met by Bots, with the following limitation which is met by Kidambi:

Art Unit: 2137

Wherein said incoming PCS is encoded in a header of said first data packet, and wherein said determining comprises decoding said incoming PCS from said header of said first data packet (Kidambi: Col 25, line 53 to Col 26, line 3 and Bots: Fig 6);

Bots discloses all the limitations of the claim except for the limitation that the source and destination addresses are decoded from the header. Kidambi discloses the idea of encoding the source and destination addresses in the header. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to encode the source and destination addresses in the header of a data packet because doing so is a commonly accepted method of effectively transmitting the source and destination addresses.

10

Claims 14,17,31,34,48, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable by Bots in view of Kisor, U.S. Patent No. 6,266,773.

As per claims 14,17,31,34,48, and 51, the applicant describes the method of claims 15 13,12,30,29,47, and 46, which are met by Bots, with the following limitation which is met by Kisor: Further comprising recording an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set (Col 3, lines 42-67); Bots discloses all the limitations of claims 13,12,30,29,47, and 46. However, Bots fails to disclose the use of recording an event in a security log. The use of a security log for recording an event 20 is disclosed by Kisor in a computer security system. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Kisor with those of Bots and add a security log for recording an event for extra security and monitoring in the system.

Response to Arguments

25 Applicant's arguments with respect to the 102(e) rejection of claim 1 under Bots have been fully considered, but they are not persuasive. Specifically, Applicant presents the following three arguments:

1) Bots does not anticipate performing the actions of the claimed invention within a *single node*

2) Bots does not change an incoming PCS to an outgoing PCS

3) Bots does not compare an incoming PCS with an IFCS, an incoming PCS with a second incoming PCS, and an outgoing PCS to a destination community set

4) Bots teaching is not equivalent to a PCS

5

Regarding 1), Applicant argues that claim 1 calls for "determining, discarding, and processing...within a single node" (lines 23-24) and that Bots teaches use of two VPN units (e.g. 250 and 252 of Fig 2). Bots discloses a network security system in which computer terminals in disparate networks may wish to communicate (e.g. device 201 in LAN A may wish to communicate with device 211 in LAN B). In order to accomplish this task in a secure fashion, Bots implements a unique firewall comprising Virtual Private Network Units (VPNUs). Thus, device 201 in LAN A may pass a packet via a router through the firewall, which may comprise VPNUs 250 and 252. If the firewall authenticates the packet, it is output to device 211. Examiner agrees that the two VPNUs are two units. However, the two VPNUs are acting as part of a single firewall entity. Without language precluding the foregoing firewall entity from meeting "a node", the claims are given their broadest reasonable interpretation (see MPEP 2111).

Regarding 2), Applicant argues that Bots does not change an incoming PCS to an outgoing PCS because Bots does not change the group membership. Such an argument is not persuasive because it is outside the scope of the claimed invention. No language in claim 1 requires a change in group membership. Claim 1 calls for changing an incoming PCS to an outgoing PCS. Bots teaches that an incoming PCS is received via a VPNU unit (e.g. 250), processed according to techniques such as encryption, authentication, and compression techniques and then output as an outgoing PCS to be received by another VPNU unit (e.g. 252). Accordingly, Bots teaches changing an incoming PCS to an outgoing PCS as required by the claims.

Regarding 3), Applicant argues that the claimed invention calls for a) comparing an incoming PCS with an IFCS, b) comparing an incoming PCS with a second incoming PCS, and c) comparing an outgoing PCS to a destination community set. Applicant believes that claim 1 is patentably distinct

because it teaches three comparisons whereas Applicant believes Bots to only teach two comparisons.

Applicant does not elaborate on which comparison(s) is deficient or how the language of the claims is believed to patentably distinguish over Bots as required by 37 CFR 1.111. Nonetheless, as indicated in the citations given in the previous action, Bots teaches that when a packet is received at a VPNU

5 interface, it is determined whether the source and destination addresses for the data packet are members of the same VPN group (e.g. Col 7, lines 1-4). Further, the data packet(s) may be discarded if it is not from an identified member of a VPN group supported by the VPNU (Col 8, lines 2-4). Thus, Bots teaches discarding a first packet if it is not a member, or a subset of, the VPN group(s) (community set(s)) acceptable for interface receipt (limitation b of claim 1).

10 Further, Bots teaches that if a data packet has an incoming PCS which matches a second incoming PCS, the data packet is processed in accordance with the encryption, authentication, and compression techniques of such VPN group, or community set (Col 6, lines 37-48). Accordingly, the data packet is readily acceptable as it is passed through the firewall from a receiving VPNU (e.g. 250) to a terminal VPNU (e.g. 252) (limitations d and e of claim 1). Finally, Bots teaches that the terminal VPNU 15 (e.g. 252) will identify the outgoing PCS via the compression, authentication, and encryption techniques to ascertain a VPN group and determine whether the packet is allowed to be transmitted to the destination community it is intended for, prior to transmitting the data packet over to the destination community (limitation f of claim 1).

4) Regarding 4), Applicant argues that Bots' teaching of a VPN group is not equivalent to a PCS. 20 Further, Applicant defines a PCS to be "the intersection of the user community or set of communities which the source node serves and the user community or set of communities which the destination node serves" (Remarks page 7). Bots "VPN group" represents an intersection of communities served by the source node and the destination node. Applicant's argument is that since a PCS **may** encompass more than one community on the source node and/or more than one community on the destination node, Bots 25 VPN group is deficient. Examiner notes that even if Bots VPN group does not encompass more than one community on the source node and/or more than one community on the destination node, such reasoning is flawed because a PCS is not defined to require an intersection of more than one community from a

Art Unit: 2137

source node and/or more than one community from a destination node, albeit a PCS **may** encompass the foregoing.

Conclusion

5 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH 10 shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should 15 be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

20 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) 25 at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


EMANUEL L. MOISE
ADVISORY PATENT EXAMINER